Amendments to the Claims

Kindly amend claims 1-3, 6-8, 10, 14, & 17-20 as set forth below. All pending claims are reproduced below, with changes in the amended claims shown by underlining (for added matter) and strikethrough/double brackets (for deleted matter).

1. (Currently Amended) Method for downloading application components from a server via a client to a multifunction smart card ~~chipcard~~, wherein the server and the client are interconnected via a distributed system, said method comprising:

a) delivery of a secret key or Session Key by the server to the client;

b) loading into the server of a sequence of commands to download an application component to the smart card ~~chipcard~~;

c) generation of a digital signature in the server using the secret key or Session Key by way of each command within the command sequence;

d) transmission of the signed command sequence as a data packet to the client;

e) unpacking of the data packet by the client and transmission of the individual commands in sequence to the smart card ~~chipcard~~; and

f) checking of the digital signature of the individual commands and execution of the commands on the smart card ~~chipcard~~ if the digital signature is correct.

2. (Currently Amended) Method in accordance with Claim 1, wherein the authentication method for generation of the Session Key is selected by:

a) transmission of a request from the server via the client to the smart card ~~chipcard~~ to transmit the smart card ~~chipcard~~ identification data stored on the smart card ~~chipcard~~;

b) reading of the smart card ~~chipcard~~ identification data from the nonvolatile memory of the smart card ~~chipcard~~ and transmission of the smart card ~~chipcard~~ identification data via the client to the server; and

c) identification from the smart card ~~chipcard~~ identification data of an authentication method by means of which a Session Key agreed between the server and the smart card ~~chipcard~~ can be generated.

3. (Currently Amended) Method in accordance with Claim 2, wherein the Session Key is determined by an authentication method comprising:

a) generation of a first random number and selection of a secret key by the server;

b) transmission of the first random number in accordance with step a) via the client to the smart card ~~chipcard~~;

c) generation of a second random number by the smart card ~~chipcard~~;

d) creation of a Session Key from the first and second random numbers and the transmitted keys;

e) encrypting the first and second random numbers and transmitting the first and second encrypted random numbers and the second random number generated by the smart card ~~chipcard~~ to the server; and

f) generation of a Session Key by the server and checking of the first and second encrypted random numbers, and the second random number with the aid of the Session Key.

4. (Original) Method in accordance with Claim 1, wherein the distributed System is an intranet or an Internet.

5. (Original) Method in accordance with Claim 1, wherein communication between the server and the client runs via SSL (Secure Sockets Layer) as the transfer protocol.

6. (Currently Amended) Method in accordance with Claim 1, wherein on the server a runtime program exists which communicates with the client and uses the keys accessible to the server as necessary, and defines the protocol specifying when which messages must be exchanged with the client and when which keys must be used; and that on the client a runtime program exists which communicates both with the smart card ~~chipcard~~ and with the server and which implements the protocol defining when which messages must be exchanged with the smart card ~~chipcard~~ and the server.

7. (Currently Amended) Method in accordance with Claim 1, wherein the smart card ~~chipcard~~ includes smart card ~~chipcard~~ identification data, the smart card ~~chipcard~~ identification data including as a minimum a smart card ~~chipcard~~ serial number and a smart card ~~chipcard~~ type.

8. (Currently Amended) Method in accordance with Claim 1, wherein the digital signature is executed by way of a symmetrical cryptoalgorithm with the aid of the Session Key agreed between the client and the server, or by way of an asymmetrical cryptoalgorithm with the aid of a private key located on the smart card ~~chipcard~~, wherein the server is in possession of the public key.

9. (Original) Method in accordance with Claim 8, wherein the symmetrical cryptoalgorithm is DES or Triple-DES and the asymmetrical cryptoalgorithm is RSA, DSA or an Elliptic Curve algorithm.

10. (Currently Amended) Method in accordance with Claim 3, wherein the secret key is derived from the smart card ~~chipcard~~ identification data and the Master Key.

11. (Previously Presented) Method in accordance with Claim 1, wherein the command sequence as a minimum comprises an Install command, one or more Load commands and a final Install command, and is stored in an Application Protocol Data Unit structure.

12. (Original) Method in accordance with Claim 1, wherein each command within the command sequence is encrypted by means of the Session Key.

13. (Original) Method in accordance with Claim 1, wherein the command sequence is a predefined sequence for a specific application which is stored in the nonvolatile memory of the server and is loaded into volatile memory of the server during the program runtime.

14. (Currently Amended) Method in accordance with Claim 1, wherein the command sequence is generated by the server program, and wherein on the server a runtime program exists which communicates with the client and uses the keys accessible to the server as necessary, and defines the protocol specifying when which messages must be exchanged with the client and when which keys must be used; and that on the client a runtime program exists which communicates both with the smart card ~~chipcard~~ and with the server and which implements the protocol defining when which messages must be exchanged with the smart card ~~chipcard~~ and the server.

15. (Original) Method in accordance with Claim 14, wherein card-specific data are integrated into the command sequence.

16. (Previously Presented) Method in accordance with Claim 13, wherein the first command within the sequence is assigned a MAC (message authentication code) with the aid of a random number and the secret key and all subsequent commands are assigned a MAC based on the MAC of the preceding command and the key.

17. (Currently Amended) Device including at least the following components:

a) Client at least including:

aa) a Browser

bb) a computer program product to execute unpacking of a data packet comprising a signed command sequence and transmission of individual commands thereof in sequence to a smart card ~~chipcard~~

cc) a reader for the smart card ~~chipcard~~

b) Server including at least:

aa) a computer program product to execute:

i) delivery of a secret code or Session Key by the server to the client

ii) loading into the server of a sequence of commands to download an application component to the smart card ~~chipcard~~

iii) generation of a digital signature in the server using the secret key or Session Key by way of each command within the command sequence

iv) transmission of the signed command sequence as the data packet to the client

bb) a nonvolatile memory to store the secret keys and the Master Key

c) Communication link between client and server.

18. (Currently Amended) Client at least including:

a) a Browser

b) a computer program product to execute unpacking of a data packet comprising a signed command sequence and transmission of individual commands thereof in sequence to a smart card ~~chipcard~~, the data packet being received from a server.

19. (Currently Amended) Client in accordance with Claim 17 further including:

c) a smart card ~~chipcard~~ reader

d) a smart card ~~chipcard~~ with a nonvolatile memory at least containing the following data:

aa) a card number

bb) a card type

cc) a secret key.

20. (Currently Amended) Computer program product stored in the internal memory of a digital computer, containing elements of software code to execute a method for downloading application components from a server via a client to a smart card ~~chipcard~~, wherein the server and the client are interconnected via a distributed system, said method comprising:

a) delivery of a secret key or Session Key by the server to the client;

b) loading into the server of a sequence of commands to download an application component to the smart card ~~chipcard~~;

c) generation of a digital signature in the server using the secret key or Session Key by way of each command within the command sequence;

d) transmission of the signed command sequence as a data packet to the client;

e) unpacking of the data packet by the client and transmission of the individual commands in sequence to the smart card ~~chipcard~~; and

f) checking of the digital signature of the individual commands on the smart card ~~chipcard~~ and execution of the commands if the digital signature is correct.

* * * * *